Naval Security Enterprise (Security Symposium) Newsletter

From the Senior Director for Security

I very much look forward to seeing you at the 2015 Naval Security Enterprise (NSE) Symposium 13 -17 April at the National Conference Center in Leesburg, Virginia. We've had an overwhelming level of support from the security community for attendance and great support from the Department. If you are attending, you'll join about 450 other security professionals to share information and best practices, learn about new security programs, and hear from and meet security leaders from the interagency and DoD. For those of you who will make it to the symposium, I request you be the "eyes and ears" for those who could not travel to Leesburg and share what you learn with your leaders and community members back at home station.

Our staff from the Security Directorate will be available in breakout meetings and in the evenings to meet with you and answer your questions. Sessions will be held Tuesday - Thursday. Each day will focus on a general theme. Day 1 will focus on Policy and will have guest speakers from DoD/DON present to discuss recent and proposed changes to Policy. Day 2 will focus on Insider Threat with guest speakers from DoD, Cybersecurity, and NCIS. Afternoons will provide breakout sessions to discuss specific topics within each security discipline. Day 3 will focus on Security Education, Training and Certification as well as hands on workshops.   This is a great opportunity for the community. I very much appreciate the support for the symposium you and your commanders have shown.

To view the NSE Security Symposium Agenda, click here.

Security Education, Training, and Awareness (SETA) and Functional Community Branch

The following topics are going to be presented at the Naval Security Symposium:

Indexing of DON Security Positions: The briefer is Tracy L. Kindle, DUSN (P) Security, assisted by Ronald Adams, Center for the Development of Security Excellence (CDSE). The breakout session provides information on the details of identifying, coding DON Security Position Descriptions, required language in security recruitment announcements and the impact of indexing on the security workforce.

Preparing for Security Professional Educational Development Program (SPēD) Certifications: The briefer is Boyd Crouse, from the Center for Development of Security Excellence (CDSE). The objective of this breakout session is to provide DON security professionals with information to prepare to take a SPēD certification exam, coordinate with your Service Program Management Office, the use of Competency Preparation Tools and the SPēD Certification Candidate Handbook. To prepare yourself for discussion during this breakout session, we recommend you access the "Prepare for Certification" link: for additional information: http://www.cdse.edu/certification/prepare.html

SPēD Certification Maintenance: The briefer is Ronald Adams, CDSE. The objective of this breakout session is to provide DON SPēD certified security professionals with information and a computer demonstration on the processes to maintain your SPēD certification. To prepare yourself for discussion during this breakout session, I recommend you access the "Prepare for Certification" link: for additional information: http://www.cdse.edu/certification/maintain-sped.html

Information Security Branch

1) Cybersecurity Panel Discussion (Dan DelGrosso-PEO EIS, Russ Smith-DONCIO, Julie Vida-OPNAV N2/N6BC, Ray Letteer-USMC C4, Neal Miller–FCC): The panel will provide their perspective on the importance of working with traditional security environment, and where the Department of the Navy is headed with new technology (Cloud, mobility to include bring your own device (BYOD), virtualization, etc.).

2) DoD Information Security Program (Ed Kaufhold – USD(I)): Provide information on developing DoD policy.

3) DON Information Security Program (Bridget DelGrosso-DUSN (P) Security): Provide information on InfoSec efforts the last couple years, developing policy, InfoSec challenges/issues, and status on the update to the Information Security Program manual.

4) Marking (Richard Avery-DSS CDSE): Focus is to provide policy requirements for marking, along with a practical exercise, to assist with conducting random sampling for marking compliance within their command as part of the annual self-inspection and identifying focus areas for initial or annual refresher training.

5) USN/USMC Mobility Initiatives (Dan DelGrosso-PEO EIS, Delores Washburn-PEO C4I, Peter Ziomek-DONCIO, LCDR Bobby Carmickle-OPNAV N2/N6BC, Ray Letteer-USMC C4, Jon Kling(SES)- Naval Reactors, Neal Miller–FCC): Panel discussion format. Presenters represent a wide range of cybersecurity experience to provide perspectives on mobility afloat, ashore, Navy reactors, resource sponsor responsibility, USMC initiatives, and DON policy. The panel will place emphasis on why the traditional security community would care about mobility. Some areas of discussion includes: Installing WI-FI hotspots on ships and how that may/may not affect classified spaces; Wireless policy (re: mobile device, laptops, etc. in classified spaces); Command Cyber Readiness Inspections (CCRI's) and the impact of mobile technology (re: is this considered on the inspection checklist); Storing, processing, transmitting information (CUI or classified) on mobile devices; Mobile capability on travel (re: hotels); BYOD (protecting the information using personal device, spillages, etc.); C&A and what risk considerations are given to information, personnel, physical and industrial security during the approval process, etc.

6) A Discussion with SSO Navy (Mark Lawton-SSO Navy): Over view of ever-changing organization structure as Naval Intelligence Activity (NIA), provide guidance on our newly acquired (from Defense Intelligence Agency) Secure Compartmented Information Facility accreditation authority and program, and discussion on common Command Security Manager – Special Security Officer communication interface issues in the fleet, address laptop and Fitbit questions. (Beneficial to attend the Cybersecurity and/or Mobility Panel Discussions to find out more on these matters).

7) Department of the Navy Information Security Program Manual (SECNAV M-5510.36) Discussion (Carmen Lanier-DUSN (P) Security, April Minor-DUSN (P) Security, Shari Belill-NAWCWD TDY to DUSN (P) Security): Brief overview of the major changes underway to the update of the DON InfoSec Program Manual (e.g., complete restructuring of the manual, self-inspection criteria, security classification guide format, new/updated exhibits, removal of Industrial Security chapter, etc.). This will be an interactive discussion with the attendees as a means to solicit recommendations/feedback for improving the guidance and/or exhibits for consideration by DUSN (P) Security when updating the manual.

8) Annual Reports-SF-311 & Self-Inspection (Carmen Lanier-DUSN (P) Security, Shari Belill-NAWCWD TDY to DUSN (P) Security): Present the fiscal year 2013-2014 comparative data, trend analysis, and common data errors for each report. Provide recommendations for improving the data provided for both reports. Also, review the draft guidance developed for the annual self-inspection report to assist Command Security Managers with assessing their program, in order to better articulate findings/recommendations/best practices to their Commanding Officer and in formal reporting to DUSN (P) Security. This will be an interactive discussion with the attendees as a means to solicit recommendations/feedback for improving annual reports submitted DUSN (P) Security either direct or via your administrative chain of command.

Physical Security Branch

Physical security across the Department of the Navy remains a challenge. Our goal during the security symposium will focus on the many facets of relationships needed to have the desired security posture needed by tenants to look at costs, defense-in-depth, and best practices to be shared for added value.

We will start the session by an overview of the DOD Physical Security Policy and Programs by USD (I). This will better inform the audience how policy is promulgated as well as how they can get their issues addressed and points of contact for better understanding of policies. We will follow this up by hosting a forum with representation from the SECNAV staff, OPNAV, USMC, CNIC and Fleet Forces Command on ways the Security Managers and other professionals can better understand organizational relationships as well as tapping into subject matter experts on their respective installations to facilitate getting the desired security posture also realizing cost savings and cooperation amongst those professionals and leadership.

Through our involvement in the SEALs Working Group, NAVFAC ESC Lockshop will provide a session focused on the security containers and other locking devices used to protect information and facilities. Professionalization and credentialing are key to our realm so we will end by having representation from the Center for the Development of Security Excellence to discuss the Physical Security Certification as well as other courses offered to give participants additional tools and insight in becoming more informed professionals. The staff is currently working on presentations covering the gamut of physical security, force protection, law enforcement and other programs. The Physical Security staff will be on hand throughout to address specific issues and questions as well as to gather suggestions and information from attendees.

Personnel Security Branch

The Personnel Security Branch will offer over 10 opportunities for updates on the Personnel Security Program. Sessions will include Department of Defense (DoD) and Department of the Navy (DON) representatives discussing DoD and DON current and future policy. Subject Matter Experts will be on-hand to discuss Security Systems currently in use to include the Joint Personnel Adjudication System (JPAS), electronic Questionnaires for Investigation Processing (eQIP), and Case Adjudication Tracking System (CATS), as well as future systems such as the Defense Information System for Security (DISS), the CATS Portal, and the Joint Verification System (JVS), the proposed replacement for JPAS.

Sessions will be held to discuss current issues, many of which have been recently addressed with the publishing of ALNAVs and Memoranda. A special session will be held for those who work with the Personnel Reliability Program. The entire Personnel Security staff will be on hand during the evening sessions to address specific issues and questions as well as to gather suggestions and information from attendees. One reminder, the Personnel Security staff will be available in the dining room during meals to have a "working meal" with attendees who care to join us.

Industrial Security Branch

The following topics are going to be presented at the Naval Security Symposium:

Industrial Security Policies Update: The following information will be presented by Ms. Valerie Heil, Chief, Industrial Security Division, Undersecretary of Defense for Intelligence (USDI). The brief will include an overview/update on DoD's Industrial Security policy, DoDM 5220.22, Volume 2 (which will replace the 1985 DoD Industrial Security Regulation); DTM 15-002, published February 11, 2015 to centralize processing of national interest determinations through Defense Security Service; and a status of revisions and approval process for DD Form 254 with instructions; and the National Industrial Security Operating Manual change 2.

Facility Security Process: The following information will be presented by Mr. Scott Dublin and Mr. Jamaar DeBoise, Defense Security Service. The Facility Clearance Process, Split Cognizance Issues, and Common Vulnerabilities and Violations found during a Security Vulnerability Assessment (SVA).

Naval Security Enterprise (Security Symposium) Newsletter

Naval Security Enterprise Branch

The OPSEC breakout session will focus on the security challenges posed by social media and other computer based outlets. Jim Magdalenski, Director of the Naval OPSEC Support Team, will lead a discussion to identify best practices, and highlight on-going efforts to achieve coordinated strategies between security, public affairs, and OPSEC professionals.

Acquisition Security Branch

The Acquisition Security Branch will offer two sessions for updates on Acquisition Security. Kate Fuster, Acquisition Security Branch Chief, DUSN (Policy), Security will provide an update on current and future initiatives. SPAWAR's Research Technology Protection Lead for Acquisition Security will provide an overview brief of acquisition security, how it relates and ties into industrial and information security, and provide insight into why cross-discipline cooperation is critical to technology protection for RDT&E and Acquisition (RDA) efforts. Subject Matter Experts will be on-hand from NAVSEA to assist in the discussions.

Sessions will be held to provide an overview on Acquisition Security in the DON and discuss current processes, procedures and initiatives surrounding Acquisition Security. The Acquisition Security Branch will be on hand during the evening sessions to address specific issues and questions as well as to gather suggestions and information from attendees.

Points of Contact:

Mailing Address:
Deputy Under Secretary of the Navy, (Policy)
1000 Navy Pentagon, Rm 4E572
Washington, DC 20350

Acquisition Security
DON_SECURITY_ACQ@NAVY.MIL
Industrial Security
DON_SECURITY_IND@NAVY.MIL
Information Security
DON_SECURITY_INFO@NAVY.MIL
Insider Threat
DON_SECURITY_INSIDER_THREAT@NAVY.MIL
Personnel Security
DON_SECURITY_PERS@NAVY.MIL
Physical Security
DON_SECURITY_PHYS@NAVY.MIL
Security Education, Training and Awareness
DON_SECURITY_SETA_US@NAVY.MIL

Useful Links:

-**Naval Security Enterprise on Navy Knowledge Online:**
https://www.nko.navy.mil/group/naval-security-enterprise/naval-security-enterprise1

- **Department of The Navy, Security Executive**:
http://www.secnav.navy.mil/dusnp/Security/Pages/Default.aspx

- **Department of The Navy, Security Education, Awareness and Training**:
http://www.secnav.navy.mil/dusnp/Security/Pages/SETACommMgmt.aspx

- **Center for Security Development of Security Excellence**: http://www.cdse.edu/index.html

- **Center for Security Development of Security Excellence, My SPeD Certifications**:
https://i7lp.integral7.com/durango/do/login?ownername=dss&usertype=candidate

- **Pearson Vue**:
https://www1.pearsonvue.com/testtaker/signin/SignInPage/DSS